



THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT *of* NEW YORK

[U.S. Attorneys](#) » [Southern District of New York](#)

Justice News

Deputy U.S. Attorney Richard Zabel Delivers Cybersecurity Keynote At Thomson Reuters Forum: “Defending Corporations And Individuals In Government Investigations”

United States ~ Thursday, December 11, 2014

We truly live in a revolutionary time. Information technology and the Internet generally has linked people together, brought the world of information to anyone with a computer and revolutionized learning, business, art, medicine and politics.

In many ways, we live in an age of enlightenment that touches more people than any other great period of knowledge advancement in history. People can access knowledge and communicate it to each other constantly even if they are on opposite sides of the globe and even if they never meet.

Now, they can do this for good reasons and they can do it for bad reasons – such as to commit crimes of all sorts – from financial crimes to acts of terrorism.

For all its good, this cyber-enabled world has also created new dangers and risks – to personal safety, to national security and to our national infrastructure and markets. We are all figuring out on the fly how to deal with these risks.

As Eric Schmidt of Google said: “The Internet is the first thing that humanity has built that humanity doesn’t understand, the largest experiment in anarchy that we have ever had.”

And through the Internet the laptop has sometimes become a weapon. Cyber criminals who have cooperated with us have told us how one person with a laptop can shut down a company, steal massive amounts of information or even disable a small country’s government from being able to communicate.

The old saying when Sam Colt invented the Colt revolver was that “God made men and Sam Colt made them equal.” Perhaps the same can be said about the laptop.

For law enforcement, not only is the technology developing fast, it is developing in ways that put information beyond the law's reach.

New technologies are being developed that are designed so as to make their information inaccessible except to the user, and this includes being inaccessible to law enforcement.

The issue I want to discuss today is whether and how much of our information and our communications traveling over the Internet should be made inaccessible to law enforcement.

Put another way, how do we balance our need for safety and the ability of the government to protect the people with the desire to maximize the privacy of our information?

The question is easier to ask than it is to answer because many of us, including the corporations that make the technology, have different views about how to balance security with confidentiality and privacy.

But we are at a point where we have to decide these issues or technology may decide them for us.

We all have to have a national discussion about where we want the lines drawn between our security and our privacy and maybe today I can tell you why many in law enforcement are concerned about this problem.

The problem of information being inaccessible to law enforcement has been described as the "going dark" problem. What does this mean?

It means that tech companies are developing innovative technology which will make information impossible or nearly impossible for law enforcement to access.

This is commonly called encryption and in this case it means encryption that is unable to be decrypted by anyone – not law enforcement and not the corporation that made the device or hosted the service. Only the user will be able to access the information.

In other words, people's communications and stored information may be made inaccessible to law enforcement even when the government can show probable cause that there is evidence of a crime committed through communications on someone's phone or through social media and law enforcement gets a warrant or court order for the information.

Law enforcement may get a search warrant but it's an exercise in futility because the evidence will not be reachable. The warrant would be served on the company and the company would say "sorry, we have no way to access the information."

Is this a real concern? I think it is.

Recently, it seems that companies have an arms race going on to develop technology and communication systems that are dark to law enforcement.

For example, just in the last few months:

1. Apple said the encryption on its latest iPhone would prevent anyone other than the user from accessing user data stored on the phone when it is locked. Even if law enforcement obtained a warrant or court order it wouldn't matter because Apple would not be able to provide access.
2. Shortly after Apple's announcement Google said it had adopted a similar encryption scheme on phones using the newest version of its Android operating system.
3. WhatsApp, which is a popular messaging service owned by Facebook, within the last month said it is now encrypting texts sent from one Android phone to another and it will not be able to decrypt the contents for law enforcement.
4. And Yahoo! is reportedly developing an encrypted email project with Google.

I should note that there are already many other social media communication platforms that are encrypted in different ways and to different degrees.

We appear to be at a moment in our society where competition among these companies is causing an eruption of encryption that could radically change law enforcement's ability to investigate and protect individuals and corporations.

The reason that encrypted systems are being developed is because the tech companies believe that their customers want to be safe from being hacked.

This has created what this corporate arms race toward complete encryption that has concerned important people in national security and law enforcement. They worry that if too much information goes dark the balance between privacy and security will tip too far.

The Director of the FBI Jim Comey has eloquently expressed concern about the increasing blackout of information from law enforcement and has said "We need our private sector partners to take a step back, to pause to consider, I hope, a change of course."

The Director of GCHQ, the British government intelligence and security organization has been more pointed. He has said about US tech companies: "However much they may dislike it, they have become the command-and-control networks of choice for terrorists and criminals, who find their services as transformational as the rest of us." He added "...[I]t can seem that some technology companies are in denial about [this]."

These are real concerns because criminals, terrorists and others who mean harm seek out whatever means of communication can keep law enforcement from seeing what they are doing.

Simply put, completely encrypted communication is a magnet for criminals.

Every day in our office we see cyber criminals and terrorists trying to find channels of communication that are shielded from law enforcement.

So let me give you a few examples:

Silk Road

The Silk Road case was one of our biggest cyber cases. We arrested Ross William Ulbricht for allegedly running a global black market for drugs, malware, firearms and other items. He was able to run it with people who acted as Administrators spread out all over the world. He basically created the Amazon.com of drugs which involved 1.2 million transactions and over 150,000 people engaging in criminal transactions with over 4,000 sellers. It involved hundreds of millions of dollars in sales and lucrative commissions for Silk Road. They used numerous methods to keep law enforcement in the dark about what they were doing including anonymizing their internet trail by operating through the TOR system and anonymizing their money trail by using Bitcoin and a Tumbler.

It was only after a tremendous investment of resources, international help around the world and some good fortune that we were able to pierce some but not all of the anonymization and encryption, and arrest Ulbricht.

Times Square

A second case is the Times Square attempted bombing case.

On Saturday, May 1, 2010, at approximately 8:00 p.m., Faisal Shahzad attempted to detonate a bomb in a sport utility vehicle in the heart of Times Square. Shahzad was arrested two days later and, after his arrest, we learned that he planned the attack with his co-conspirators, who were members of the terrorist group TTP. He described how he and his co-conspirators set up a completely secure and encrypted line of communication so they could communicate and formulate the plan securely even while he was in the United States and his co-conspirators were in Pakistan. These encrypted conversations included operational

Communications, for example, about the purchase of the SUV used to house the bomb, and the posting of videos which claimed responsibility for the attempted bombing immediately afterward.

El-Hanafi and Hasanoff

Wesam El-Hanafi and Sabirhan Hasanoff were two naturalized U.S. citizens from Brooklyn arrested in 2010. From 2007 through late 2009, they provided extensive support to al Qaeda. They were involved in conducting surveillance of domestic targets, including the New York Stock Exchange, for a possible terrorist attack.

But El-Hanafi's highest value to al Qaeda was his technical sophistication and computer expertise. El-Hanafi formerly worked as an information technology specialist at an investment bank and had received extensive training in computer security. In February 2008, El-Hanafi traveled from his home in Dubai to Yemen, to meet with two senior terrorist operatives. While in Yemen, El-Hanafi taught the senior terrorist operatives how to communicate covertly over the Internet by employing advanced encryption. El-Hanafi then developed other encrypted means of communication including encrypted emails.

ISIS

Those are some past cases. More recently, it's been reported that ISIS is using all sorts of established and new social media to spread its message. Obviously, any of those media that are

or become completely encrypted will just make any law enforcement action that much more difficult.

I raise these cases not because they involve any specific technology but because they show what we see every day – that people with bad intent want to be able to be completely encrypted so law enforcement can't reach them. Some of them succeed and some of them don't but the question is how easy and available do we want to make it for them to do this?

Do we want complete encryption to become the norm?

Everyone needs to discuss this because drawing the appropriate line between security and privacy is right at the heart of what citizens in the United States expect of their Government. They want to be free, they want to enjoy privacy and be left alone but they also want to be safe.

People have to decide on how that gets balanced.

Back to US Companies

There are different points of view in this debate.

On the one hand, many tech companies, and many individuals, will argue that US companies are leading the way in innovating completely private channels of communication and that this is a good thing. They say this is what their customers want and the companies need to provide complete encryption to compete effectively.

Those are important arguments that need to be listened to.

As is the fact, that in other parts of the world there are people fighting for freedom who benefit from having closed channels of communication and information that repressive governments can't penetrate.

There is also the argument that if you engineer system so law enforcement can access the information you are making those systems vulnerable and everyone is more susceptible to being hacked.

On the other hand, law enforcement officials and many individuals will argue that creating widespread secret channels of communication may be more an abdication of responsibility than an innovation of significance by these companies, that most citizens do not feel they need privacy to be an absolute, impenetrable wall to law enforcement –which it never has been in the history of this Nation – and that there are too many dangerous people who are the true consumers who want to communicate beyond the reach of the law.

There is also the argument that complete encryption creates dangers that outweigh the protection it provides.

Furthermore, while I am a big believer in competition, the argument that US companies cannot compete as effectively if they don't create fully encrypted communication systems and devices, does not really answer the question of where we want the line drawn between the reach of the law and privacy.

There are many things in the United States that we don't allow companies to do that harms their ability to compete, but that we consider fundamental to corporate responsibility in our society. We don't allow companies to pollute freely, we don't allow them to make unsafe or toxic products, and we don't allow them to deny their workers certain basic rights and entitlements.

All of those restrictions impose costs and may hinder the competitiveness of companies, but we have agreed as a society that these costs are outweighed by the social utility they produce.

What companies are really saying is they can make more money if they can market fully encrypted devices or services but as I've just described there are limits to the profit motive especially when it bumps up against safety.

There are also limits to privacy. Law enforcement will generally access information it needs through a search warrant, or sometimes other legal process.

It has been accepted by our country since its founding that while the 4th Amendment to the US Constitution protects the privacy of its citizens, it does not wall them off absolutely from law enforcement.

Even the most sacrosanct and private of places – a person's home –can upon a proper showing and with court approval be searched and evidence can be seized. As the 4th Amendment says:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

If the founders of this country – who from hard experience were skeptical and mistrustful of authority – allowed for judicial review for homes to be searched and evidence to be seized in order to protect the people, how can it be said that allowing devices and communication channels to be searched is unreasonable?

Are we really at the point where we are placing our phones and our computers beyond the Constitution, even when we ourselves, our houses, our papers and our effects are not?

Are we now exalting our smartphones and emails over our homes? Are we saying our digital homes can't be searched even when our actual homes can be?

That is a choice we could all make but it comes with a lot of risk, and it needs to be discussed more fully than it has been.

Courts:

One way the issue of privacy is protected is of course in the courts.

But the decision to create broad technology that does not even allow the possibility of a search warrant being used can only lead one to conclude many corporations must mistrust the courts to police the appropriate line between privacy and law enforcement's efforts to obtain evidence.

That mistrust is misplaced.

The courts have shown they are vigilant guardians of privacy concerns and the effect new technology has on privacy.

In many, many cases, courts have imposed a higher burden on law enforcement because the judges thought privacy concerns required it because of the effect of new technologies.

Let me give two examples from the Supreme Court:

1. Just this this past summer in *Riley v. California*, the Supreme Court unanimously decided it would not allow the warrantless search of the information in a cell phone seized from a defendant incident to arrest.

For decades, well-established precedent had allowed searches of property in the defendant's possession when he was arrested with no need for a search warrant. In *Riley*, the Court broke from this long precedent of warrantless searches because it specifically recognized that cell phones were different than other property; they contained so much personal and private information that the Court felt a warrant should be required.

Chief Justice Roberts, writing for the Court, said: "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans the privacies of life."

So the Court adjusted its search incident to arrest doctrine to take account of new technology and its privacy implications and said: from now on law enforcement -- you need a warrant for the phone.

2. Let's stay with the Supreme Court for another example. In 2012, the Court decided *United States v. Jones* in which the Justices determined that the use of a GPS device that law enforcement attached to the defendant's car to monitor his movements for four weeks required a warrant even though the car's movements were not private in any way as they were always visible to the public.

--the majority focused on the need for a warrant because the device was placed on the car, which was a trespass

--but five Justices also said in two different concurrences that new GPS technology allowed such lengthy, continuous surveillance by law enforcement that it implicated privacy concerns and therefore should require a warrant under the 4th Amendment.

--Justice Alito in concurrence with three other Justices wrote that "dramatic technological change may lead to periods in which popular expectations [of privacy] are in flux and may ultimately produce significant changes in popular attitudes."

--he then added that sometimes these issues may ultimately require legislation

Congress:

Of course, the line between privacy and security will not even reach the Courts if there is no information to search.

If the information is unavailable then those who make the technology will be drawing the line for all of us.

So while some of the national discussion regarding law enforcement, new technology and privacy can take place in the courts, the bigger issue of what we all believe law enforcement should have access to is a discussion that has been ongoing between law enforcement and the corporations developing encrypted products.

That is a good and important discussion but it has not yet yielded consensus and both sides may have difficulty appreciating each other's concerns.

Law enforcement should not overreach about what it needs, and should also recognize that if it does overreach, abuse its power or exaggerates, it will lose credibility and the ability to reach agreement with the industry.

But corporations too have responsibilities to be reasonable and engage in discussing the real consequences of what they are doing. For example, when the CEO of Apple says as he did in October:

"If law enforcement wants something, they should go to the user and get it. It's not for me to do that."

Well, that is not a real solution. For anyone who has been involved in law enforcement, the user is often the bad guy, the terrorist, or the cyber-criminal and you can't go to the user, first because you may not be able to reach him or identify him if he's abroad or evading law enforcement, and second, if you have to go to the user you can't do any covert and ongoing proactive investigation which in serious cases you will want to do.

Saying that law enforcement should go to the user to get your information is like saying you should never do a wiretap but rather should always get a bad guy to consent to his phone calls being monitored.

Imagine if that had been law enforcement's only option over that last few decades. We'd be nowhere on organized crime, to use just one example.

Now, I don't think the CEO of Apple said that because he doesn't care about law enforcement concerns. Of course he does, and I'm sure just like all of us he wants the right balance between safety and privacy to be struck. I just think the dialogue needs to be better so everyone understands what is doable and what is not, and CEOs need to understand law enforcement concerns just like law enforcement needs to understand the CEO's limitations in his marketplace.

As we have seen recently with the hacking assaults on our financial institutions and SONY, and the constant drumbeat of intrusions into many other companies, corporations too have been and will be on the victim side of cyber-crime.

They will want us to pursue and catch criminals who hack into their systems and it will be very dissatisfying to them – just as it is to any victim of a crime – if we have to say there is nothing we can do because the trail is completely encrypted.

So, if the courts are not presented with these issues and the dialogue between law enforcement and technology companies is too slow then it will likely be for Congress to act.

We have been down this road before and Congress acted, although the issues were narrower and simpler.

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA). The law required that switches in digital telephone networks be built wiretap-enabled – so they would not be dark.

That law is outdated now as switched networks have faded in importance and IP-based communications predominate.

But in 1994 the will of the people, as expressed through Congress, was that these communications should not be dark and that reasonable privacy could accommodate law enforcement being able to listen in on calls.

I'm not sure the will of the people has changed.

We may need to have Congress speak to that same issue in its new form today. This would bring clarity to the issue for law enforcement and the tech. It would also presumably allow the people speak through their representatives as to where they want the lines drawn between their privacy and their security.

Let me end by saying--

This Golden Age of information and communication technology has brought us to an important social moment. Lines are being drawn and re-drawn between privacy and security. What is a reasonable expectation of privacy is evolving with the transformative technology we use.

The United States tech industry is leading the way. I hope we will also lead the way in striking the right balance in these technologies between cybersecurity and cyber-privacy.

All of this implicates law enforcement's ability to protect people and we can't afford to ignore that and not make choices about how we want to live with this technology.

In the end we should be making a choice about the limits we impose on our technology and not, through inattention, have technology impose its limits on us.

USAO - New York, Southern

Updated May 13, 2015